Mạng không an toàn
Phần 2: Sống lâu với 'sửa nhanh'

Cuộc sống dài lâu của một giao thức Internet được 'sửa' nhanh từ 1989 để lại chỗ bị tổn thương dữ liệu cho những kẻ chuyên chặn cướp

Video: Xem tài liệu gốc

Tác giả Craig Timberg viết cho tờ Washington Post, xuất bản: 31/05/2015

Dịch sang tiếng Việt: Lê Trung Nghĩa, letrungnghia.foss@gmail.com

Dịch xong: 05/07/2015

Bản gốc tiếng Anh:

http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/

Net of insecurity
Part 2: The long life of a ‘quick fix’

The long life of a quick ‘fix’ Internet protocol from 1989 leaves data vulnerable to hijackers

Watch video: See on the original post

Story by Craig Timberg for The Washington Post, published 05/31/2015

Vào thời điểm 2 kỹ sư ngồi xuống ăn trưa cùng nhau ở Austin, những cố gắng gia tăng của Internet đã trở nên khốc liệt. Từng là mới mẻ cho các nhà khoa học máy tính, mạng bây giờ đã bùng nổ về kích cỡ, tròng trành hơn bao giờ hết gần với một bức tường toán học khó khăn với một trong những giao thức cơ bản nhất của Internetl.

Khi viễn cảnh hệ thống sụp đổ lờ mờ, người ta đã bắt đầu đưa ra vội vàng các ý tưởng cho một giải pháp đằng sau một chiếc khăn ăn bẩn vì nước xốt cà chua. Rồi cái thứ 2. Rồi cái thứ 3. “Giao thức 3 chiếc khăn ăn”, như những người sáng tạo ra nó đùa bỡn đặt tên cho nó, có thể sớm cách mạng hóa Internet. Và dù đã có các vấn đề còn rơi rớt lại, các kỹ sư đã thấy sự sáng tạo của họ như một sự “vọc” hoặc “lời giải nhanh”, tiếng lóng cho một sự khắc phục tạm thời sẽ được thay thế ngay khi lựa chọn thay thế tốt hơn hiện diện.

Đó từng là vào năm 1989.

Hơn 1/4 thế kỷ sau đó - khoảng thời gian mà đã thấy sự sụp đổ của bức tường Berlin, sự nổi lên của điện thoại thông minh và sự bùng nổ của việc đột nhập - “giao thức 3 chiếc khăn ăn” vẫn còn chỉ dẫn hầu hết giao thông đường dài trên mạng toàn cầu bất chấp nhiều năm cảnh báo căng thẳng gia tăng về các vấn đề an toàn sống còn. Giao thức 3 chiếc khăn ăn đã trở thành một lời giải nhanh mà không bao giờ chết.

“Các giải pháp ngắn hạn có xu hướng ở lại với chúng ta rất lâu. Các giải pháp dài hạn có xu hướng không bao giờ xảy ra”, Yakov Rekhter, một trong các kỹ sư đã sáng tạo ra “giao thức 3 chiếc khăn ăn” đã nói. “Đó là những gì tôi đã học được từ kinh nghiệm này”.

Internet có thể xuất hiện như được thiết kế một cách tao nhã như một chiếc ô tô đua khi nó ngâm chúng ta trong các thế giới tiêu dùng của âm thanh và hình ảnh. Nhưng là gần hơn với một tập hợp các lời giải nhanh - nhiều Frankenstein hơn là Ferrari - điều đó tồn tại vì chúng làm việc, hoặc ít nhất làm việc đủ tốt.

Các hậu quả diễn ra trên khắp không gian mạng mỗi giây mỗi ngày, khi các tin tặc khai thác các hệ thống cũ kỹ được bảo vệ tồi để mưu đồ bất lương, ăn cắp và gián điệp ở mức độ chưa bao giờ có khả năng trước đó. Các lỗi mà chúng khai thác thường được biết rõ và cổ xưa theo các khái niệm công nghệ, sống sót chỉ vì một thiên hướng rộng rãi của nền công nghiệp cho việc vá đối với các vấn đề hơn là thay thế thứ mục nát đó.

“Bạn đang ở trong cái làng của các tin tặc (Hackerville) ở đây trên

Câu chuyện của Craig Timberg
Các minh họa của **Harry Campbell**

Video của **Julio Negron**

Xuất bản 31/05/2015

Tạo ra Internet bị tổn thương: Câu chuyện này là phần 2 của dự án nhiều phần về các chỗ bị tổn thương vốn dĩ của Internet và vì sao chúng có thể không bao giờ được sửa.

Phần 1: Câu chuyện Internet đã trở nên dễ bị tổn thương đến thế bằng cách nào

Phần 3: Các tin tặc đó đã cảnh báo Internet có thể trở thành một thảm họa về an toàn. Đã không ai nghe cả.

Internet. Chấm hết”, Randy Bush, một nhà khoa học máy tính chuyên về an toàn định tuyến, nói. “Tất cả những thứ đó thiếu nguyên tắc chính thức... Nó là sơn và trát”.

Câu chuyện về “giao thức 3 chiếc khăn ăn” đó, còn được biết một cách chính thức hơn như là Giao thức Cửa ngõ Biên giới, hoặc BGP.

Ở mức cơ bản nhất của nó, BGP giúp các bộ định tuyến quyết định cách gửi các dòng dữ liệu khổng lồ qua lưới khổng lồ các kết nối tạo nên Internet. Với số lượng vô hạn định các con đường có khả năng - vài đường chậm và uốn khúc, vài đường khác nhanh và thẳng - BGP trao cho các bộ định tuyến thông tin chúng cần để chọn ra một con đường, thậm chí dù hoàn toàn không có tấm bản đồ của Internet và không có cơ quan nào có trách nhiệm về việc định tuyến của nó cả.

Sự tạo ra BGP, điều dựa vào các mạng cá nhân liên tục chia sẻ thông tin về các liên kết dữ liệu có sẵn, đã giúp Internet tiếp tục sự tăng trưởng của nó thành mạng toàn cầu. Nhưng BGP cũng cho phép các đường bị cắt khổng lồ của dữ liệu bị “chặn cướp” (hijacked) bởi hầu hết bất kỳ ai với các kỹ năng và sự truy cập cần thiết.

Lý do chính là BGP, giống như nhiều hệ thống khóa trên Internet, được xây dựng để tự động tin cậy những người sử dụng - thứ gì đó có thể làm việc trong các mạng nhỏ hơn nhưng lại để cho mạng toàn cầu là chín muồi cho các cuộc tấn công.

Ảnh: Xem tài liệu gốc

Yakov Rekhter, một trong những kỹ sư đã sáng chế ra Giao thức Cửa ngõ Biên giới - BGP (Border Gateway Protocol), nói các nhà vận hành mạng sẽ miễn cưỡng triển khai các biện pháp an toàn mạnh hơn cho tới khi họ thấy các lợi ích nặng hơn các chi phí. (Yana Paskova của The Washington Post).

Hệ thống danh giá

Các vụ chặn cướp đã trở thành các sự kiện thường ngày mà thậm chí các chuyên gia phải vật lộn để giải thích: Điều gì đã tạo ra giao thông giữa 2 máy tính ở Denver chọn một đường quanh co 7.000 dặm qua Iceland? Làm thế nào có thể một công ty duy nhất của Pakistan đánh sập được YouTube? Vì sao dữ liệu nhạy cảm tiềm tàng của Lầu 5 góc lại đã từng chảy qua Bắc Kinh?

Đối với những câu hỏi đó, có các câu trả lời kỹ thuật. Nhưng tất cả chúng đều dẫn tới thực tế này: BGP chạy trên hệ thống danh giá, cho phép dữ liệu được kéo và đẩy qua khắp thế giới theo các cách thức tò mò, theo mệnh lệnh của những người chủ huyền bí.

Các cảnh báo về các rủi ro vốn dĩ trong BGP hầu hết là kỳ dị hệt như bản thân giao thức đó. “Tôi đã biết rằng an toàn định tuyến từng là một vấn đề”, nhà khoa học máy tính của Đại học Columbia Steven M.

Bellovin nói. “Nhìn điều này bằng khái niệm là khá dễ và ngay thẳng. Phân loại nó ra theo kỹ thuật lại khá khó”.

Rekhter, một người nhập cư vào Mỹ, người từng chơi trong ban nhạc rock dưới tầng ngầm ở Liên Xô, nói an toàn “đã không có thậm chí trên bàn” khi ông ngồi xuống với người đồng sáng tạo ăn nói nhỏ nhẹ của mình, Kirk Lougheed, ăn trưa trong quá trình một hội nghị kỹ thuật vào tháng 01/1989.

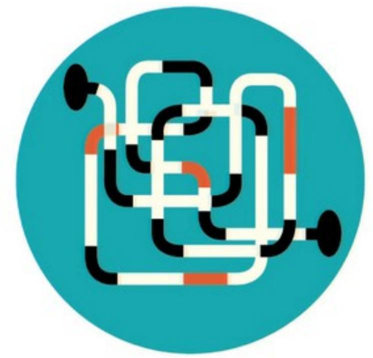
Đây từng là một kỷ nguyên khi mà các vụ đột nhập từng là hiếm và số người là khiêm tốn. Lougheed đã nhớ lại: “Trong những ngày đầu của Internet, để làm cho thứ gì đó làm việc được từng là mục tiêu hàng đầu. Đã không có khái niệm là mọi người có thể sử dụng điều này để làm những điều độc hại... An toàn từng không phải là vấn đề lớn”.

Vấn đề lớn của ngày đó từng là khả năng Internet có thể bị sập. Một sự ngưng trệ trong sự mở rộng điên khùng của nó có thể làm tổn thương tới những người sử dụng mạng và lợi nhuận của các công ty cung cấp các dịch vụ và phụ tùng. Rekhter khi đó đã làm việc cho người khổng lồ máy tính IBM; Lougheed từng là một nhân viên sáng lập của Cisco, người tạo ra phần cứng kết nối mạng.

“Chúng tôi cần bán các bộ định tuyến. Và chúng tôi đã có một động lực kinh tế mạnh để chắc chắn cuộc vui này có thể tiếp tục”, Lougheed nói. “Khi Yakov và tôi đã chỉ ra một giải pháp và nó dường như làm việc được, mọi người hoàn toàn có thiện chí chấp nhận nó vì họ đã không có thứ gì khác”.

Đã có những nỗ lực khác đang diễn ra để xây dựng các giao thức định tuyến. BGP đã thắng vì nó từng là đơn giản, đã giải quyết được vấn đề trong tay và đã chứng minh được sự linh hoạt đủ để giữ cho các dữ liệu chảy trong khi Internet tăng gấp đôi về kích cỡ, gấp đôi nữa và nữa và nữa. Các mạng khắp thế giới đã ôm lấy giao thức đó, trao cho nó cái góc cạnh nó chưa từng bao giờ buông ra.

Một khi các công nghệ được triển khai rộng, chúng trở nên hầu như không thể thay thế vì nhiều người sử dụng - bao gồm cả các khách hàng trả tiền của các công ty công nghệ - dựa vào chúng và từ chối mua các phần cứng hoặc phần mềm mới đắt tiền. Kết quả có thể là một thứ được xây dựng với công nghệ lỗi thời, cứ lớp này xây trên đỉnh lớp kia. Nó dường như giống các hầm ngân hàng quan trọng nhất ngày nay ngồi trên nền của rơm và bùn vậy.



Giao thức Cửa ngõ Biên giới - BGP (Border Gateway Protocol)

Các quy tắc giúp các bộ định tuyến router quyết định làm thế nào gửi dữ liệu qua Internet. Các mạng dựa vào sự truyền thường xuyên các thông điệp BGP để xác định cách tốt nhất dịch chuyển hàng tỷ con đường có khả năng tới cái đích theo ý muốn đối với 1gói dữ liệu. Nó có các điểm yếu về an toàn đáng kể mà 1 phiên bản được cập nhật, gọi là BGPSEC, đang cố gắng sửa.

Pakistan đánh sập YouTube

Trong một thế giới trực tuyến thịnh hành không có an toàn, các vấn đề với BGP hầu hết là trùng hợp. Để nếm trải vì sao, hãy tới thăm tầng 3 một khối văn phòng buồn tẻ vùng ngoại ô Hanover, N.H. Ở đó, Doug Madory trải qua những ngày tuyệt vời của anh ta với những điều điên khùng đã từng xảy ra với Internet - sự sáng tạo của con người ngày càng thách thức sự hiểu biết của con người.

Madory và các đồng nghiệp của anh ở Dyn, một hãng nghiên cứu hiệu năng trực tuyến, cố làm cho có ý nghĩa của sự điên rồ bằng việc gửi đi 450 triệu đường theo dõi mỗi ngày để dõi xem Internet đang chạy. Ông so sánh các con đường lần vết - các tập hợp bit nhỏ dữ liệu lỏng lẻo trên trực tuyến - tới các mẩu bụi mà các chuyển động của chúng tiết lộ các sức mạnh mạnh hơn trong công việc.

Một ngày gần đây, Madory đã thử chỉ ra vì sao vài giao thông Internet của Trung Quốc lại chảy qua Bạch Nga. Một ngày khác, đó từng là giao thông Internet của nước Anh - bao gồm cả vài giao thông có ý định cho Cơ sở Vũ khí Nguyên tử của quốc gia đó, một phòng thí nghiệm vũ khí hạt nhân - chảy qua Ukraine. Trong cả 2 trường hợp, Madory đã chỉ ra, có lẽ là kết quả của các sai lầm, nhưng đã không có cách gì để khẳng định chắc chắn cả.

“Điều này xảy ra suốt ngày”, Madory, một cựu sỹ quan Không Quân thích đàn đúm, tóc ngắn và hợp mốt, với đôi kính vuông, nói. “Bất kỳ điều gì cũng có thể xảy ra, và nó thường xuyên thế”.

Chệch đường giao thông Internet, thậm chí chệch đường không cố ý, có thể là lý do của các vấn đề khổng lồ qua mạng. Có lẽ hầu hết các sự cố nổi tiếng tới vào tháng 02/2008, khi nhà cung cấp dịch vụ Internet Pakistan đã cố khóa YouTube sau khi chính phủ nghi sự miêu tả của một video xúc phạm nhà tiên tri Muhammad.

Khi công ty Pakistan đó đã cố gắng triển khai lệnh của chính phủ, nó đã phạm một sai lầm trong việc thiết lập cấu hình các thông điệp BGP của nó tới phần còn lại của Internet. Kết quả là hầu hết giao thông toàn cầu của YouTube đã được gửi tới Pakistan. Sức ép dữ liệu tràn ngập các máy chủ ở đó và đã đánh sập YouTube trong 2 giờ đồng hồ.

Nhưng vấn đề lớn nhất là tiềm tàng đối với các vụ chặn để cướp cố ý.

Một tin tặc không rõ tên tuổi đã cố chiếm quyền kiểm soát giao thông được định sẵn cho hơn một tá công ty Internet, bao gồm cả Amazon và

Alibaba, trong một loạt các cuộc chặn để cướp ngắn giữa tháng 2 tới tháng 5/2014. Mục tiêu là để ăn cắp các đồng tiền bitcoin trực tuyến. Vào lúc cuộc đột nhập đã bị phát hiện, tiền bitcoins trị giá 83.000 USD đã biến mất - huyền bí lấy từ giao thông Internet bị chặn để cướp - theo báo cáo của Dell Secure Works.

Những cuộc tái định tuyến như vậy có thể để lại bằng chứng trong mạng mà có thể được lần vết bằng các dịch vụ phân tích như Dyn (trước đó được gọi là Renesys), nhưng những kẻ tấn công tinh vi phức tạp nhất có thể dấu mặt sự nhận diện của họ khi điều khiển BGP, các chuyên gia nói. Và thậm chí khi nguồn gốc chặn để cướp là rõ ràng, thì có thể là khó khăn để phân biệt được động lực.

Sự làm trệch hướng của Trung Quốc đối với giao thông quân đội Mỹ trong 18 phút vào tháng 04/2010 là một trong những sự cố được nghiên cứu cẩn thận nhất trong lịch sử lâu đời của sự không an toàn của BGP, nhưng các chuyên gia vẫn còn tranh luận liệu nó có từng là cố ý hay không. Nó đã bắt đầu khi China Telecom, một người khổng lồ viễn thông do nhà nước quản lý, đã gửi đi một thông điệp BGP nói sẽ cung cấp các đường tốt nhất cho hàng chục ngàn mạng trên thế giới, bao gồm cả 16.000 mạng từ Mỹ.

Với không hệ thống nào tại chỗ kiểm tra tính xác thực của thông điệp BGP từ China Telecom, các bộ định tuyến trên khắp thế giới đã bắt đầu gửi dữ liệu tới Bắc Kinh, ở phía bên kia thế giới. Trong số những mạng bị ảnh hưởng có các site của chính phủ Mỹ cho Lục quân, Hải quân (Navy), Không quân và lính biển (Marines).

Thông điệp BGP đã được sửa cho đúng, và Dyn và các nhóm nghiên cứu khác đã kết luận rằng có khả năng đó là một sự cố. Vâng hình như dễ cho việc chặn để cướp - và thiếu các bảo vệ có hiệu quả chống lại một sự lặp lại - đã cảnh báo các quan chức Mỹ.

Chính phủ Trung Quốc có thể đã sử dụng chiến thuật đó để phân tích dữ liệu quân sự về các mật khẩu, các giao tiếp truyền thông được mã hóa và hơn thế nữa. Hoặc Trung Quốc có thể đã sao chép tất cả các dữ liệu cho phân tích sau này. Một vụ chặn để cướp BGP, các chuyên gia cảnh báo, là giống như một vụ đột nhập vào steroids, cho phép kẻ trộm dữ liệu trong một phạm vi rộng khác thường.

Có một khả năng nguy hiểm khác được che dấu trong BGP, những gì Madory gọi là "khả năng đầy kinh hoàng" mà vài mạng - có lẽ ở vào thời điểm khi các thế lực thù địch quốc tế đang nhảy vào không gian

mạng - tuyên bố kiểm soát cố ý các phân khúc của Internet mà không thuộc về nó.

Một động thái như vậy có thể gây lúng túng cho các bộ định tuyến trên thế giới, điều có thể phải chọn giữa các tuyên bố sống còn với các khối y hệt các địa chỉ Internet. Toàn bộ mạng, không có khả năng nhận ra sự đúng đắn trong số lượng các tuyên bố cạnh tranh nhau, có thể gây rạn nứt trong các lãnh địa của đối thủ.

Điều này có thể tương đương với "lựa chọn hạt nhân" của Internet, một sự leo thang thù địch mà là có khả năng về mặt kỹ thuật nhưng có lẽ khó tưởng tượng được - ít nhất vào thời gian khá hòa bình. Hậu quả cho việc vận hành của Internet như một mạng toàn cầu không liền mạch có thể là không có khả năng đảo ngược.

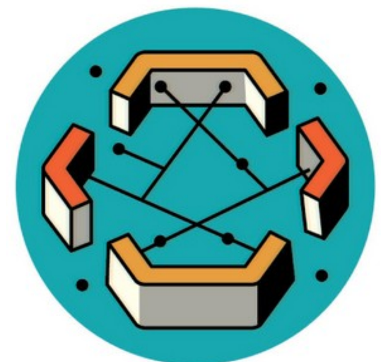
"Nó có thể là dạng chỉ ủy thác", Madory nói. "Điều gì giữ cho nó khỏi việc ủy thác? Không gì cả".

'Đầu gối nằm sâu trong các con cá sấu'

Những người tạo ra BGP từng chỉ là những người đầu tiên sáng tạo để phác thảo các ý tưởng ban đầu của họ nhanh chóng và thô sơ, chỉ để tinh chỉnh các ý tưởng đó sau này qua các kiểm thử trong thế giới thực. Tốc độ, sự lanh lẹ và tính thức dụng từng là các dấu tiêu chuẩn của phát triển Internet trong những thập niên đầu của nó, khuyến khích cả sự tăng trưởng theo hàm mũ và khả năng của nó để cạnh tranh với các công nghệ đối thủ mà sự phát triển của chúng từng chính thức hơn và - có lẽ không thể tránh khỏi - cũng buồn tẻ hơn.

David D. Clark, một nhà khoa học ở MIT, người đã giám sát sự phát triển của giao thức Internet nhiều năm, đã nắm bắt được ý tưởng đó trong một trình bày được dẫn trích năm 1992, nói: "Chúng tôi từ chối các ông vua, các tổng thống và biểu quyết. Chúng tôi tin tưởng vào sự đồng thuận dân dã và mã chạy được" - nghĩa là các giải pháp mà làm việc và được ôm lấy một cách rộng rãi.

Tiếp cận này đã không luôn khuyến khích việc lên kế hoạch dài hạn thậm chí cho các mối đe dọa an toàn như Internet đã cuốn hút một vũ trụ những người sử dụng gia tăng, bao gồm cả nhiều động lực của họ vốn dĩ hoàn toàn khác với các động lực của các nhà nghiên cứu hàn lâm trước hết đã ôm lấy công nghệ kết nối mạng hiện đại trong những năm 1970 và 1980.



ARPANET

Một mạng máy tính tiên phong được Cơ quan các Dự án Nghiên cứu Tiên tiến - ARPA (Advanced Research Projects Agency) của Lầu 5 góc xây dựng. Được thiết lập vào năm 1969, nó cuối cùng đã liên kết hơn 100 trường đại học và cơ sở quân sự, trở thành người báo trước cho Internet ngày nay.

Vào thời gian Rekhter và Lougheed đã tạo ra BGP, đã có vài sự cố nghiêm trọng. Nhưng dạng của việc đột nhập bất biến, lợi ích cao hành hạ thế giới trực tuyến ngày nay đã chưa bắt đầu. Ý tưởng về chiến tranh không gian mạng vẫn còn là một câu chuyện khoa học viễn tưởng.

Các vấn đề mà các kỹ sư kết nối mạng đối mặt, ngược lại, từng là thực tế và ngay lập tức. ARPANET - tiền thân quan trọng nhất của Internet, được cơ quan nghiên cứu của Lầu 5 góc tạo ra - từng suýt bị đánh sập sau 2 thập kỷ. Các mạng chính khác từng vật lộn với vấn đề gọi là "vòng lặp", trong đó các dữ liệu xoay quanh theo các vòng điên loạn, ngốn các tài nguyên tính toán trước khi bốc hơi hoàn toàn.

Vâng vấn đề lớn nhất từng là giới hạn chặt chẽ của toán học về kích cỡ Internet, như được viết trong nguyên mẫu đầu tiên cho BGP, gọi là Giao thức Cửa ngõ từ Ngoài vào - EGP (Exterior Gateway Protocol). Nó có thể điều khiển chỉ một số cố định các địa chỉ mạng. Thậm chí một địa chỉ thêm có thể làm cho các hệ thống thành phi trực tuyến.

"Mỗi người đều có đầu gối nhúng quá sâu trong các con cá sấu mà họ chỉ cần có thứ gì đó nhanh cùng nhau", Noel Chiappa, một nhà nghiên cứu kết nối mạng đã nghỉ hưu, nói. "Họ đã không có thời gian để nhìn về lâu dài".

BGP từng là một sự cải tiến ngay lập tức, cho phép Internet tiếp tục phát triển bùng nổ trong khi thiết lập giai đoạn cho sự hiện diện của World Wide Web sớm sau đó. Rekhter và Lougheed, trong số những người khác, vẫn còn ngạc nhiên về sáng tạo của họ đã được chứng minh kéo dài tới thế nào. Họ đã tưởng tượng BGP phân loại qua ít ngàn con đường có khả năng trên Internet. Bây giờ là hàng trăm lần nhiều hơn thế.

Tương lai đó, Rekhter nói, "từng vượt qua sự tưởng tượng điên rồ nhất của chúng tôi".

Ảnh: Xem tài liệu gốc

Kirk Lougheed, một trong những đồng sáng tạo BGP và một nhân viên sáng lập của Cisco, nói an toàn sẽ được tiến hành nghiêm túc khi sự hiếu vắng nó trở thành một "chi phí đáng kể cho việc làm kinh doanh. ... Tại thời điểm này, mọi người chỉ đang vá con đường họ đi qua, giữ một bước trước những kẻ xấu". (Nick Otto của The Washington Post).

Các mạng không có bản đồ

Internet là một mạng của các mạng, từng mạng trong số chúng có sự hiện hình vật lý, trong thế giới thực trong các rack (tủ có các khe cắm máy) các máy chủ nằm trong các trung tâm dữ liệu ở các nơi như Ashburn, Va., and Santa Clara, Calif. Các mạng cũng có bất động sản trực tuyến khối các địa chỉ IP mà chúng kiểm soát, biểu thị bản vá

không gian mạng của chúng.

Các mạng lớn nhất, được những người khổng lồ viễn thông vận hành như Verizon và AT&T, thường mang các tải dữ liệu nặng nhất. Chúng là các hãng hàng không của không gian mạng, có khả năng nhanh chóng lôi kéo giao thông các khoảng cách xa qua các đường cáp quang trước khi trao nó cho các mạng nhỏ hơn, vận hành giống với các con đường lân cận. Các mạng nhỏ hơn đó, như hệ thống máy tính của một trường đại học hoặc một nhà cung cấp Internet địa phương, thường phân phối giao thông ở cái chân cuối cùng của nó cho các máy tính cá nhân hoặc các thiết bị khác như các điện thoại thông minh.

Kết quả của kiến trúc này - với nhiều mạng các kích cỡ khác nhau vâng không thực thể duy nhất nào có trách nhiệm về định tuyến giao thông - là một mớ hỗn độn khổng lồ các kết nối mà đưa ra số các đường hầu như vô hạn định để gửi các dữ liệu giữa 2 điểm. BGP giúp các bộ định tuyến chọn một đường, thậm chí dù các mạng luôn thay đổi và các con đường phổ biến thường bị cản trở giao thông.

Vấn đề: Không có bản đồ. Các bộ định tuyến sử dụng BGP đưa ra các quyết định định tuyến dựa vào thông tin được các người hàng xóm của họ trong không gian mạng cung cấp, điều tới lượt nó thu thập thông tin từ những người hàng xóm của họ trong không gian mạng, và cứ như thế. Điều này làm việc tốt miễn là thông tin - có trong các thông điệp được gọi là "các quảng cáo" BGP - là chính xác.



Địa chỉ IP

Mã số khác biệt biểu thị kết nối duy nhất tới Internet. Giống hệt như địa chỉ đường vật lý, một địa chỉ IP là cơ bản để làm cho các gói dữ liệu tới được các địa chỉ đích có chủ đích.

Bất kỳ thông tin sai nào cũng có thể lan truyền hầu như tức thì khắp Internet vì không có đường nào để kiểm tra được tính thực chất, hoặc thậm chí sự nhận diện, của những ai đưa ra các quảng cáo đó. Một mạng mà phân phối thông tin tồi có thể được thông báo lặp đi lặp lại, và những người vận hành các mạng khác có thể cố gắng khóa những người làm phiền như vậy thông qua một kỹ thuật gọi là "lọc". Nhưng các bảo vệ như vậy thường là hơn cả phù hợp.

Một vấn đề rõ ràng như vậy, Lougheed nói, có thể không bao giờ bị chịu lỗi trong thế giới biết rõ về an toàn hơn như ngày nay. "Nếu ai đó tới với một cử chỉ mà không biết trước sự lừa gạt, thì họ sẽ bị đánh và gửi ngược về bàn vẽ", ông nói.

Liệu lý do là sự lừa gạt cố ý hay một sự cố ngẫu nhiên, các kết quả là y hệt nhau: giao thông Internet bị trệch hướng, thường hàng ngàn dặm. Đôi khi cuối cùng nó tìm được đường của nó tới đích đúng, chỉ gây ra sự chậm trễ truyền. Đôi khi các dữ liệu bị các tin tặc ăn cắp.

Đôi khi nó chỉ biến mất hút trong không gian mạng, hệt như ở Tam giác Bermuda.

Xung lượng không dừng lại được

Dù Rekhter và Lougheed đã không tập trung vào mối nguy hiểm này khi họ đã tạo ra BGP, thì ít nhất một kỹ sư kết nối mạng khác đã lo lắng về nó. Radia Perlman, từng được gọi là "người mẹ của Internet" vì sáng tạo của bà giao thức kết nối mạng quan trọng khác, đã viết một luận án tiến sỹ tiên đoán trước cho MIT vào năm 1988, năm trước khi Rekhter và Lougheed đã tạo ra BGP. Bà đã tiên đoán rằng một giao thức mà phụ thuộc vào tính lương thiện và chính xác của những người hàng xóm trong không gian mạng sẽ được coi là không an toàn.

Bà và vài nhà bình luận đã ưa thích hơn các lựa chọn thay thế mà trao cho các bộ định tuyến một bản đồ của hầu hết các kết nối quan trọng nhất - tương đương với một đồ thị toàn cầu các liên kết trong không gian. Perlman cũng đã ưa thích hơn sử dụng mật mã để thẩm tra các nhận diện các mạng, hạn chế tiềm tàng việc lừa dối và hạn chế thiệt hại khi có các sai lầm.

Nhưng BGP đã có xung lượng không thể dừng lại được. "Một khi mọi người đã quen với nó, thì có sự kháng cự cực kỳ lớn để thay thế nó", Perlman nói, người đã lấy làm tiếc rằng các kỹ sư làm việc về các lựa chọn thay thế tốt hơn đã không xúc tiến được ngay. "Không may, nhóm khác đã không thực sự cảm thấy ý nghĩa của sự cấp bách. Điều chỉ là những người của BGP đã triển khai thứ gì đó trước".

Rekhter và những người khác đã tiếp tục cải tiến BGP, triển khai phiên bản cuối cùng của giao thức đó vào năm 1994. Các cuộc chặn để cướp dữ liệu đã bắt đầu rồi, làm rõ nhu cầu về một giao thức thay thế an toàn hơn, nhưng nhiều năm làm việc đã thất bại để tạo ra một giao thức có thể thay cho BGP.

"Tất cả các đề xuất đó đã chết trong rượu", Tony Lim, một kỹ sư đã từng làm việc với Rekhter trong việc tinh chỉnh BGP, nói.

Mối lo về các rủi ro an toàn vốn dĩ của BGP đã gia tăng sau ngày 11/09/2001, các cuộc tấn công khủng bố. Nhà khoa học máy tính Vinton G. Cerf, một trong những kiến trúc sư sáng lập quan trọng nhất của Internet, và một người tiên phong về kết nối mạng khác đã ra nhập, Stephen Kent, trong việc thúc giục chính phủ hành động. Họ đã

gặp cố vấn đặc biệt của Tổng thống George W. Bush về an ninh không gian mạng, Richard A. Clarke, ở Tòa nhà Văn phòng Điều hành Eisenhower, bên cạnh Nhà Trắng.

Clarke sớm triệu tập một cuộc họp với các lãnh đạo công nghiệp hàng đầu với hy vọng nhắc nhở hành động, nhưng họ đã không chia sẻ sự cấp bách của Cerf và Kent - hoặc của Clarke. Nhiều năm trôi qua mà không có tiến bộ đáng kể nào.

“Về cơ bản họ nói, 'Đó không phải là vấn đề lớn'”, Kent nhớ lại. “Nên chúng tôi đã thử, nhưng mọi người chỉ thổi chúng đi”.

Clarke đã nói trong một cuộc phỏng vấn gần đây rằng ông từng không ngạc nhiên vì phản ứng thờ ơ từ giới công nghiệp công nghệ. Ông đã được nhắc về những rủi ro của BGP vài năm trước từ một nhóm tin tặc ở Boston có tên là L0pht, nhóm đã cảnh báo nhấn mạnh với các quan chức liên bang rằng Internet là không an toàn tới mức độ gây sốc.

Điều đó đã dẫn Clarke mang các mối lo về BGP tới các quan chức khác của Nhà Trắng và các tay chơi chính trong giới công nghiệp. Trong cuốn sách năm 2008 của ông “Chính phủ của bạn đã quên bạn”, ông đã mô tả cuộc viếng thăm một lãnh đạo hàng đầu giới công nghiệp, người mà, khi Clarke đã thúc ép về các rủi ro của BGP, đã yêu cầu ông để viết tên lên một mẩu giấy.

“Tôi không nghĩ tôi bao giờ đó nghe về điều đó”, Clarke đã nhớ lại người lãnh đạo đó nói trong cuốn sách của ông, “nhưng nếu bạn nói có chỗ bị tổn thương với nó mà ảnh hưởng tới các bộ định tuyến của chúng tôi, thì tôi sẽ kiểm tra nó”.

Clarke đã thể hiện sự ngạc nhiên trong cuốn sách của ông rằng người đứng đầu một công ty mà “đã kiếm được bạc tỷ” trong việc sản xuất ra các sản phẩm đã sử dụng BGP đã không nghe về nó, vâng Clarke đã không nêu tên của vị giám đốc đó.

Nhưng trong cuộc phỏng vấn gần đây với tờ Washington Post, Clarke đã nói rằng cuộc gặp là từng diễn ra với John Chambers, lãnh đạo lâu đời của Cisco, hãng khi đó từng là một trong những công ty có giá trị nhất thế giới và là tay chơi áp đảo trong thị trường các bộ định tuyến đã sử dụng BGP để giao tiếp truyền thông.

Cisco đã từ chối bình luận.

Ảnh: Xem tài liệu gốc

Vào năm 1989, Yakov Rekhter và Kirk Lougheed đã phác họa lên 3 chiếc khăn ăn kế hoạch của họ cho việc định tuyến dữ liệu qua Internet. “Giao thức 3 chiếc khăn ăn”, chính thức được biết tới như là Giao thức Cửa ngõ Biên giới (BGP), từng có ý định sẽ là sự khắc phục nhanh nhưng vẫn điều hành cách mà các dòng giao thông đường dài qua không gian mạng. Sự tái tạo của Rekhter các bức phác họa đó được thấy ở đây.

'Không ai từng mua cả'

Sự hoài nghi của giới công nghiệp có gốc rễ trong ý tưởng rằng an toàn từng là vụ cược tồi cho kinh doanh. Không ai thích bị đột nhập, nhưng các công ty về pháp lý đã không tin về những thiệt hại. Các biện pháp bảo vệ, trong khi đó, chịu chi phí mà ít người muốn bỏ tiền ra, như các tính năng bị giới hạn, hiệu năng bị chậm hoặc các thẻ giá cao hơn cho các phụ kiện và phần mềm.

Các công ty mà đã trải nghiệm với các sản phẩm đã có các tính năng an toàn bổ sung thêm, như mã hóa được xây dựng sẵn, đã thấy ít lợi ích từ các khách hàng đã có các lựa chọn thay thế rẻ hơn, dễ hơn, như Robert Metcalfe, người sáng lập ra 3Com, nguyên là nhà sản xuất phần cứng mạng, nói.

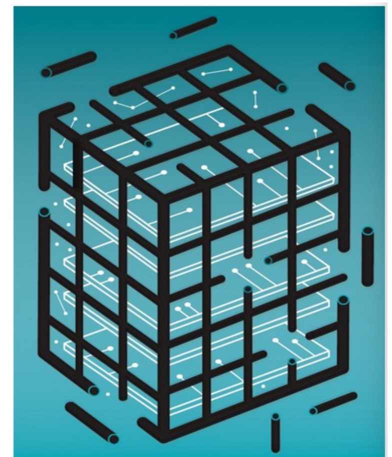
“Không ai muốn mua các phiên bản an toàn”, Metcalfe nói. “Chúng tôi xây dựng nó, và chúng tôi đã cố bán nó, và không ai mua cả”.

Tốc độ hành động để sửa lỗi BGP đã gia tăng sau sự cố vào tháng 04/2010 có liên quan tới giao thông của quân đội Mỹ chảy qua Bắc Kinh. Một sự thúc giục lớn đã tới từ Bộ An ninh Nội địa (DHS), nó đã bỏ ra 8 triệu USD trong 4 năm qua trong nỗ lực phát triển và triển khai công nghệ BGP an toàn. “Đây là một phần các nỗ lực liên tục của chúng tôi để nâng cao toàn bộ an toàn các dịch vụ Internet cốt lõi mà mọi người sử dụng”, người phát ngôn của DHS, S.Y. Lee, nói.

Bước đầu tiên tiến tới an toàn BGP tốt hơn từng là một hệ thống mới các khóa mật mã an toàn cho các mạng, cho phép chúng xác thực các nhận diện của chúng trong không gian mạng và làm rõ các mạng nào chúng thường điều khiển giao thông.

Một khi một hệ thống như vậy hiện diện, thì có thể là khó cho một nhà cung cấp Internet Pakistan, ví dụ, kêu về giao thông của YouTube. Các bộ định tuyến router có thể đơn giản bỏ qua các thông điệp BGP rởm, kết luận chúng là có lỗi.

Nhưng để cho các nhà vận hành mạng tham gia vào là khó. Nhiều người triển khai rồi các bộ lọc mà giới hạn sự phát hiện các thông điệp BGP rởm. Tiếp cận đó chỉ đưa ra sự bảo vệ một phần, nhưng nó là dễ dàng hơn so với việc sử dụng các khóa mật mã. Nhiều nhà vận hành mạng cũng là khá khi tiến hành các bước tiếp xa hơn trong việc áp dụng một giao thức định tuyến an toàn mới gọi là BGPSEC để thay thế BGP.



Ảnh: Xem tài liệu gốc

Dữ liệu đi qua Internet như thế nào

Nháy vào ảnh để xem hình đồ họa.

Nhiều kỹ sư kết nối mạng nói rằng BGP, thậm chí sau 1/4 thế kỷ và với bất tận các vụ chặn để cướp, vẫn còn được cho là rất thành công hơn là thất bại. Nó đã giúp Internet trở thành một mạng thực sự toàn cầu, liền mạch, công nghệ giao tiếp truyền thông thay đổi thế giới trong đó không nhà chức trách nào áp đặt được cho ai có thể sử dụng nó và như thế nào.

Cách phi tập trung hóa đó của việc ra các quyết định, điều là cơ bản hơn cho Internet so với bất kỳ giao thức nào, cũng có nghĩa là các cải tiến về an toàn đòi hỏi nhiều hành động cá nhân của các mạng, các nhà vận hành các site và những người sử dụng. Từng người phải cân nhắc giá trị của sự thay đổi, rồi tiến hành. Hoặc không.

“Có một chi phí có liên quan tới tiến hành an toàn. Và câu hỏi là: Ai sẽ trả tiền?”, Rekhter nói, bây giờ đã nghỉ hưu. “Trừ phi các nhà vận hành [mạng] có thể thấy rằng những lợi ích thường sẽ vượt qua các chi phí, nếu không họ sẽ không triển khai nó”.

Lougheed, cũng vậy, là một người hoài nghi. “Nếu thiếu an toàn trở thành một chi phí đáng kể để tiến hành kinh doanh, thì nhiều người sẽ quan tâm trong việc sửa vấn đề đó. Vào lúc này, mọi người chỉ vá con đường mà họ đi qua nó, giữ một bước trước các kẻ xấu”.

Mức độ nhiệt thành cho việc triển khai các biện pháp an toàn BGP mới quả thực khác nhau rộng lớn khắp thế giới. Ở châu Âu và Trung Đông cộng lại, hầu như 9% các mạng đã thực hiện bước đầu tiên có các khóa mã hóa cho việc nhận viện bản thân họ trong không gian mạng. Nam Mỹ làm tốt hơn, với 24% các mạng có các khóa mật mã. Bắc Mỹ và châu Phi làm tệ hơn nhiều, với ít hơn 1%. Bức tranh tổng thể toàn cầu, bao gồm cả châu Á, là 5%.

Mục tiêu, tất nhiên, là 100%. Không ai biết bao giờ sẽ có được.

“Bạn có thể cười khi thấy con số 5%, nhưng bạn có biết cần bao nhiêu công việc để đạt tới được đó không?” Sharon Goldberg, một giáo sư thỉnh giảng về khoa học máy tính ở Đại học Boston, người nghiên cứu về các vấn đề an toàn định tuyến, nói.

Đối với việc mất bao lâu triển khai đầy đủ, bà đã huỵch toẹt ra, “Có thể là 5 hay 10 hay 20 năm nữa, tôi không biết”.

Còn bây giờ - sau nhiều năm cảnh báo của Perlman, Bellovin, Kent, Clarke và nhiều người khác - có lẽ số liệu thống kê nói lên nhiều nhất là số % giao thông Internet hiện được hệ thống mới đảm bảo an toàn với các khóa mạng mật mã: là 0.

Thừa nhận

Câu chuyện của **Craig Timberg**
Các minh họa của **Harry Campbell**

Video của **Julio Negron**, **Jorge Ribas**